Deutscher Bundestag **Drucksache 19/11445**

19. Wahlperiode 09.07.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Frank Sitta, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/10952 –

Digitale Souveränität

Vorbemerkung der Fragesteller

Die Bundesregierung hat die digitale Souveränität als wichtiges Ziel für ein innovatives und wirtschaftlich starkes Deutschland und Europa benannt. Da Souveränität in diesem Kontext die unabhängige Selbstbestimmung in Bezug auf digitale Systeme und Daten meint, ist der Begriff der „digitalen Souveränität“ sowohl für Staaten als auch für Einzelpersonen anwendbar. Für den Bereich der Staaten steht die digitale Souveränität auf mehreren Säulen, darunter beispielsweise die alleinige Kontrolle über die Speicherung, Weitergabe und Nutzung von Daten oder auch die Fähigkeit, Hardware-Komponenten zu entwickeln, herzustellen und zu kontrollieren. Da eine vollständige digitale Souveränität für Staaten in aller Regel weder realistisch erreichbar noch erstrebenswert ist, muss bei den entscheidenden Aspekten der Souveränität immer eine Abwägung zwischen Kosten und Nutzen stattfinden. So ist beispielsweise die vollständige Neuentwicklung für ein bereits über Dritte verfügbares Tool unter Umständen sehr kostenintensiv, kann aber möglicherweise trotzdem einen großen Mehrwert haben, wenn dadurch beispielsweise betroffene sensible Daten auf europäischen oder deutschen Servern gehalten werden können.

Zur Entwicklung entsprechender Strategien entstanden unter Beteiligung der Bundesregierung im Rahmen des Nationalen IT-Gipfels 2015 in der Fokusgruppe 1 das Papier „Leitplanken Digitaler Souveränität“ (www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf?__blob=publicationFile&v=1) und im Rahmen des Digital-Gipfels 2018 in der Fokusgruppe „Digitale Souveränität in einer vernetzten Gesellschaft“ das Papier „Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen“ (www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5). Während sich das Papier des Nationalen IT-Gipfels bezüglich der Definition von digitaler Souveränität noch auf die Verhinderung unausweichlicher Abhängigkeiten und die Feststellung beschränkt, dass digitale Souveränität auf verschiedenen Pfeilern ruht, entwickelt das Papier aus dem Jahr 2018 die Definition des Begriffs weiter und ergänzt sie um eine Entscheidungshilfe. Darin wird ein Schichtmodell digitaler Souveränität beschrieben, welches den Fokus auf die

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Wirtschaft und Energie vom 3. Juli 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Fähigkeit legt, „technologische Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren und durch andere Komponenten zu ergänzen“ (S. 3 des Papiers).

Die immer wieder festgestellten international unterschiedlichen Datenschutzniveaus (vgl. beispielsweise die Cloud-Speicherung der Bodycam-Daten) und international unterschiedlichen Zugriffsmöglichkeiten durch Sicherheitsbehörden und Geheimdienste (vgl. beispielsweise die Diskussion zu Huawei oder aktuelle Pläne des Bundesministeriums des Innern, für Bau und Heimat zu Hintertüren in verschlüsselten Messengern) zeigen nach Ansicht der Fragesteller die Notwendigkeit auf, sich mit dem Thema der digitalen Souveränität zu befassen.

1. Inwiefern fühlt sich die Bundesregierung an die von ihr auf dem IT-Gipfel 2015 und dem Digital-Gipfel 2018 mit ausgearbeiteten Papiere zur digitalen Souveränität gebunden?

Für die Bundesregierung stellen die Projekte, Initiativen und Publikationen der Gipfel-Plattformen wichtige Beiträge zur Gestaltung der Digitalisierung in Deutschland und Europa dar. Sie schätzt sie insbesondere deshalb, weil sie Verständigungen vieler wichtiger Akteure der digitalen Wirtschaft, Wissenschaft und Gesellschaft sind. Die in den Papieren enthaltenen Handlungsempfehlungen werden von den zuständigen Ressorts sorgfältig geprüft und es werden – soweit möglich – geeignete Umsetzungsmaßnahmen ergriffen. Dabei werden auch und gerade die Aspekte der digitalen Souveränität sehr ernst genommen.

2. An welchen Stellen sind Projekte zur Förderung des Ziels digitaler Souveränität in der „Umsetzungsstrategie der Bundesregierung zur Gestaltung des digitalen Wandels“ festgehalten?

   Mit welchen konkreten Zielen und Maßnahmen sind die Projekte hinterlegt?

3. Hat sich das Digitalkabinett der Bundesregierung bereits mit Fragestellungen im Bereich der digitalen Souveränität beschäftigt?

   a) Falls ja, mit welchen, und mit welchem jeweiligen konkreten Ergebnis?

      Von welchen Ressorts wurden die Fragestellungen eingebracht?

   b) Falls nein, wann wird sich das Digitalkabinett mit welchen Fragestellungen beschäftigen?

      Welche Wünsche wurden aus den verschiedenen Ressorts schon dahingehend geäußert?

Die Fragen 2 und 3 werden gemeinsam beantwortet.

Im Papier der Fokusgruppe „Digitale Souveränität in einer vernetzten Gesellschaft“ der Digital-Gipfel-Plattform „Innovative Digitalisierung der Wirtschaft“ mit dem Titel „Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen“ vom Dezember 2018 wird richtigerweise darauf hingewiesen, dass der Begriff „Digitale Souveränität“ umfassend zu verstehen ist und viele Komponenten auf die Stärkung der digitalen Souveränität eines Landes, seiner Wirtschaft, Gesellschaft und Wissenschaftslandschaft abzielen. Daher kann keine erschöpfende Liste von Maßnahmen aufgestellt werden, die auf die Stärkung der digitalen Souveränität abzielen. Prinzipiell sollen alle Maßnahmen der Umsetzungsstrategie und Fragestellungen unter Befassung des Digitalkabinetts zu einer stärkeren Souveränität Deutschlands in Digitalfragen beitragen.

Beispiele für Maßnahmen, die in Bezug zu den einzelnen Punkten stehen, die in den im Rahmen der jeweiligen Digitalgipfel ausgearbeiteten Papiere aufgeführt werden, sind in den Antworten zu den Fragen 5, 8 und 11 zu finden.

4. Werden staatliche Infrastrukturen mit dem Ziel der Erreichung maximaler digitaler Souveränität aufgebaut?

a) Falls ja, in welchen Bereichen, und in welchem Umfang?

Wann sollen diese jeweils fertiggestellt sein?

b) Falls nein, warum wird auf staatliche Infrastrukturen in den einzelnen Bereichen verzichtet?

Der Frage entsprechend werden Maßnahmen, die im Wesentlichen von der Wirtschaft getragen und durch den Staat flankiert werden, nicht aufgeführt.

Staatliche Infrastrukturen zur Gewährleistung der digitalen Souveränität Deutschlands werden beispielsweise in den folgenden Bereichen aufgebaut:

Im Bereich der Forschung wird der Aufbau einer Nationalen Forschungsdateninfrastruktur (NFDI) vorangetrieben. Derzeit oft dezentral, projektförmig und temporär gelagerte Datenbestände von Wissenschaft und Forschung sollen im Rahmen der NFDI für das gesamte deutsche Wissenschaftssystem systematisch erschlossen werden. Zentrales Ziel ist die Etablierung und Fortentwicklung eines übergreifen-den Forschungsdatenmanagements, das Anbieter und Nutzer in einer übergeordneten Struktur zusammenbringt. Die NFDI soll Standards im Datenmanagement setzen und als digitaler, regional verteilter und vernetzter Wissensspeicher Forschungsdaten nachhaltig sichern und nutzbar machen.

Zum Schutz der IT- und Cybersicherheit innerhalb der Bundesregierung und Bundesverwaltung wurden folgende Maßnahmen ergriffen:

- Entwicklung einer eigenen Bundescloud;
- Verschlüsselung leitungsgebundener elektronischer Kommunikation mit SINA-Technologie, sichere mobile Kommunikation mit Smartphones und Tablets durch die Lösungen SecurePIM (iOS), SecuSuite (Android, BlackBerry) und SINA (Windows, Linux) , wobei alle Produkte „Made in Germany“ sind;
- Betrieb eines sicheren Übertragungsnetzes für die Kommunikation der öffentlichen Verwaltung, gemäß der Netzstrategie 2030 der öffentlichen Verwaltung im Eigenbetriebsmodell durch einen internen Netzdienstleister. Die Bundesregierung sichert sich hiermit Kontroll-, Durchsetzungs- und Wahlmöglichkeiten bei Planung, Aufbau und Betrieb von Netzinfrastrukturen;
- Dienstekonsolidierung, um bis Ende 2025 die Infrastrukturen der Bundesverwaltung durch standardisierte, harmonisierte und großflächig nutzbare IT-Lösungen zu unterstützen, die über definierte Schnittstellen miteinander verzahnt und hochgradig aufeinander abgestimmt sind. Für jeden Dienst existieren dabei maximal zwei unterschiedliche IT-Lösungen.

5. Wie fördert die Bundesregierung die von ihr in den „Leitplanken Digitaler Souveränität“ erkannten Schlüsselkompetenzen in den Bereichen der Entwicklung offener Standards, der Software-Kompetenzen, der Hardware-Kompetenzen und der IT-Sicherheit?

   Welche konkreten Maßnahmen hat die Bundesregierung ergriffen, um die von ihr erkannten Schlüsselkompetenzen für die öffentliche Hand zu fördern?

Die in den Papieren enthaltenen Handlungsempfehlungen von den zuständigen Ressorts sorgfältig geprüft und es werden – soweit möglich – geeignete Umsetzungsmaßnahmen ergriffen. In Bezug auf die in dem genannten Papier aufgeführten Schlüsselkompetenzen hat die Bundesregierung zu diesem Zeitpunkt beispielsweise folgende Maßnahmen ergriffen:

1. Software-Kompetenzen

Die Entwicklung von Software-Kompetenzen stellt einen Schwerpunkt der Technologieförderung des Bundesministeriums für Bildung und Forschung (BMBF) dar. Zentrale aktuelle Themen sind insbesondere Künstliche Intelligenz, um die KI-Strategie der Bundesregierung umzusetzen, Software-intensive eingebettete Systeme, Softwarearchitekturen für den sicheren Datenaustausch sowie die Entwicklung eines Betriebssystems für das Internet der Dinge.

Digitale Kompetenzen und Kenntnisse sind in der dualen Aus- und Fortbildung verankert. Neben technikoffenen Formulierungen in den Verordnungstexten identifiziert das Bundesministerium für Wirtschaft und Energie (BMWi) fortlaufend gemeinsam mit der Praxis den Bedarf für neue Anforderungen. So werden beispielsweise bei der derzeit laufenden Modernisierung der vier dualen IT-Berufe die Themen IT-Sicherheit, Datensicherheit, Datenschutz und personale Kompetenzen in allen Berufsprofilen nochmals deutlich gestärkt.

Darüber hinaus organisiert der Deutsche Industrie- und Handelskammertag im Bereich der dualen Ausbildung in Zusammenarbeit mit der Bundesregierung an mehreren Industrie- und Handelskammertagen den „Praxisdialog: Duale Ausbildung digital“. Das von der Bundesregierung geförderte RKW-Kompetenzzentrum führt in Zusammenarbeit mit Kammern, Verbänden und Wirtschaftsförderungen das Projekt Digitalisierungsscouts durch.

Auch unterstützt die Bundesregierung die Unternehmen bei der digitalen Weiterbildung der bestehenden Belegschaft. Beispielsweise unterstützt die Bundesregierung kleine und mittlere Unternehmen durch die Förderung des Kompetenzzentrums Fachkräftesicherung, welches Informationsangebote u.a. auch mit Blick auf die Digitalisierung bereitstellt. Sie fördert überbetriebliche Berufsbildungszentren und unterstützt durch das Programm Mittelstand-Digital kleine und mittlere Unternehmen und Handwerksbetriebe beim digitalen Wandel ihrer Geschäftsprozesse und stellt mit einem bundesweiten Netzwerk von 25 „Mittelstand 4.0 – Kompetenzzentren“ auf die Bedürfnisse des Mittelstandes zugeschnittenes Know-how bereit.

2. Hardware-Kompetenzen

Das BMBF unterstützt die Entwicklung von Hardware-Kompetenzen insbesondere durch Umsetzung des Forschungsrahmenprogramms „Mikroelektronik aus Deutschland – Innovationstreiber der Digitalisierung“. Mit der „Forschungsfabrik Mikroelektronik Deutschland“ und den „Forschungslaboren Mikroelektronik“ investiert das BMBF seit 2017 massiv in die deutsche Mikroelektronik-Forschung

an Forschungseinrichtungen und Hochschulen und treibt deren Vernetzung voran. Im Rahmen eines „wichtigen Vorhabens von gemeinsamem europäischem Interesse“ (IPCEI) investiert die Bundesregierung zudem 1 Mrd. Euro in die europäische Mikroelektronik-Industrie.

Zur Hardware-Entwicklung insbesondere im Bereich der Sensorik und Aktorik, tragen darüber hinaus die Forschungsprogramme „Photonik Forschung Deutschland“ sowie „Technik zum Menschen bringen“ bei.

3. IT-Sicherheit

Mit dem Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit, „Selbstbestimmt und sicher in der digitalen Welt“, fördert die Bundesregierung den Aufbau von Kompetenzen und die Entwicklung von Technologien für sichere und vertrauenswürdige IT-Systeme. Dazu wurden insbesondere drei Kompetenzzentren für die IT-Sicherheitsforschung in Saarbrücken (CISPA), Darmstadt (CRISP) und Karlsruhe (KASTEL) aufgebaut. Diese haben sich zu international anerkannten Forschungs- und Beratungszentren entwickelt und die Entstehung von Innovationsökosystemen für die IT-Sicherheit ermöglicht.

Mit der Initiative „IT Security made in Germany“ des Verbandes „TeleTrusT – Bundesverband IT-Sicherheit e. V.“ gib es darüber hinaus eine privatwirtschaftliche Initiative, welche unter anderem auf die Förderung der Zusammenarbeit von deutschen Unternehmen bei Ausschreibungen und die Unterstützung von Exportaktivitäten abzielt.

Zur Unterstützung von IT-Sicherheit „made in Europe“ werden derzeit die Errichtung eines sogenannten Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und die Einrichtung eines Netzwerks nationaler Koordinierungszentren auf europäischer Ebene im Trilogverfahren verhandelt.

Das BMWi unterstützt über die Initiative „IT-Sicherheit in der Wirtschaft“ auf Seiten der Anwender Unternehmen darin, ihre IT-Sicherheit zu verbessern. Insbesondere kleine und mittlere Unternehmen sollen für das Thema sensibilisiert werden. Dazu werden konkrete, praxisnahe und verständliche Handlungsanleitungen und Maßnahmen erarbeitet und den Unternehmen kostenfrei zur Verfügung gestellt, die sich gut in den Unternehmensalltag integrieren lassen. Seit Beginn des Jahres 2019 wird die Initiative „IT-Sicherheit in der Wirtschaft“ deutlich ausgebaut.

Das Bundesministerium des Innern, für Bau und Heimat (BMI) und der Bundesverband der Industrie (BDI) haben im September 2018 das „Cyberbündnis mit der Wirtschaft“ ins Leben gerufen. Im Rahmen der Kooperation sollen u. a. Produkte und Dienstleistungen und insbesondere Schlüsseltechnologien für kritische Geschäftsprozesse, die zur Wahrung der digitalen Souveränität der deutschen Wirtschaft essentiell sind, jedoch aktuell nicht von nationalen oder europäischen Unternehmen angeboten werden, identifiziert werden. Sodann soll die Projektrealisierung/Entwicklung umgesetzt werden, wobei der BDI hier nicht tätig wird. Die Finanzierung soll nach einem Aufruf zur Co-Finanzierung schwerpunktmäßig durch die Wirtschaft mit einer beihilferechtlich zulässigen Beteiligung des Bundes (Zuwendung) erfolgen.

Auch mit der Agentur für Innovation in der Cybersicherheit wird das BMI gemeinsam mit dem Bundesministerium der Verteidigung in Zukunft einen Beitrag zur Erhöhung der digitalen Souveränität leisten. Die Cyberagentur ist ein Bau-

stein der Bundesregierung zum Schutz der Bürgerinnen und Bürger im Cyberraum. Sie wurde bereits im Koalitionsvertrag zwischen CDU, CSU und SPD 2018 angekündigt, im August 2018 im Kabinett beschlossen und bettet sich in die Hightech-Strategie 2025 der Bundesregierung ein. Die Cyberagentur soll ambitionierte Forschungs- und Entwicklungsvorhaben initiieren, finanzieren und koordinieren, sofern sie strategische Vorteile für die innere und äußere Sicherheit versprechen.

Aufgabe der Cyberagentur wird es sein, Innovationen zu identifizieren und konkrete Aufträgen für die Entwicklung von Lösungsmöglichkeiten zu vergeben. Sie plant, steuert und priorisiert einzelne Programme und führt sie zusammen.

4. Offene Standards:

Innerhalb der Informations- und Kommunikationstechnik der Bundesverwaltung spielt die Verwendung von offenen, nicht proprietären Standards und Formaten eine wichtige Rolle. In diesem Kontext werden auch Kollaborationsmodelle zwischen den Standardisierungsorganisationen und Open-Source-Initiativen geprüft. Hierbei handelt es sich um einen stetigen Prozess.

6. Welche Maßnahmen hat die Bundesregierung ergriffen, um die Marktsichtbarkeit deutscher Unternehmen der IT-Sicherheitswirtschaft durch öffentliche Auftraggeber als Referenzen zu erhöhen?

   Welche Probleme ergeben sich nach Kenntnis der Bundesregierung insbesondere für die mittelständische IT-Sicherheitswirtschaft, wenn diese sich an der Ausschreibung öffentlicher Aufträge beteiligen will?

Es wird zunächst auf die Antwort zu Frage 5 verwiesen.

Auch im Bereich der öffentlichen Beschaffung ist das Thema IT-Sicherheit von zunehmender Bedeutung. Allerdings ist bei der Vergabe öffentlicher Aufträge bei einem Auftragswert oberhalb der EU-Schwellenwerte das auf europarechtlichen Vorgaben beruhende Vergaberecht nach dem Gesetz gegen Wettbewerbsbeschränkungen (GWB) durch die öffentlichen Auftraggeber zu beachten, unabhängig vom fachlichen Inhalt des Auftrags. Gemäß § 97 Absatz 1 der GWB sind öffentliche Aufträge und Konzessionen im Wettbewerb und im Wege transparenter Verfahren zu vergeben. Dabei sind die Teilnehmer an dem Vergabeverfahren grundsätzlich gleich zu behandeln. Bei der Vergabe von Aufträgen mit einem Auftragswert unterhalb der EU-Schwellenwerte gelten vergleichbare Regelungen, wie beispielsweise § 2 der Unterschwellenvergabeordnung. Das Vergaberecht ermöglicht es auch, Anforderungen an die IT-Sicherheit etwa in der Leistungsbeschreibung zu stellen, was innovativen Unternehmen der IT-Sicherheitswirtschaft zugutekommt. Gleichzeitig schreiben die vergaberechtlichen Regelungen auch vor, dass bei der Durchführung der Vergabeverfahren mittelständische Interessen vornehmlich zu berücksichtigen sind. Insbesondere gilt das Gebot der Aufteilung von Aufträgen in Lose sowie das Verbot, unangemessen hohe Anforderungen an die Eignung von Unternehmen zu stellen. Vor diesem Hintergrund hat die Bundesregierung keine Hinweise, dass es für mittelständische IT-Sicherheitsunternehmen Hindernisse bei der Vergabe öffentlicher Aufträge gäbe.

7. Wie viele und welche öffentlichen Aufträge hat die Bundesregierung im Bereich der IT-Sicherheit seit 2015 vergeben, die das Ziel verfolgen, ein Signal für IT-Sicherheit „made in Europe“ zu setzen?

   An wen sind die Aufträge vergeben worden?

Der Bundesregierung ist nicht bekannt, dass öffentliche Aufträge vergeben wurden, die explizit das Ziel verfolgen, ein Signal für IT-Sicherheit „made in Europe“ zu setzen.

8. Mit welchen konkreten Zielen und Vorhaben hinterlegt die Bundesregierung die folgenden Forderungen aus den „Leitplanken Digitaler Souveränität“ und welche konkreten Maßnahmen hat sie diesbezüglich bereits ergriffen:

   a) Grundlage für souveränes Handeln ist ein sicherer digitaler Raum;

   b) Europas Wirtschaft, Staat und Bürger müssen in die Lage versetzt werden, vertraulich und geschützt in digitalen Netzen zu kommunizieren;

   c) es darf keine Hintertüren oder sonstigen Kanäle geben, über die Daten unbefugt eingesehen, kopiert oder verändert werden können;

   d) der bewusste Einsatz von Security-Referenzprojekten in Heimatmärkten hat hohe Signalwirkung;

   e) die ENISA (European Network and Information Security Agency) muss als Kooperationsplattform für Cyber-Security gestärkt werden;

   f) die Förderung der Verfügbarkeit offener Standards als innovationsfördernder Gestaltungsrahmen muss insbesondere durch den Einsatz in Wirtschaft und öffentlicher Verwaltung gefördert werden;

   g) die öffentliche Hand sollte mit einem „Cloud First“-Programm eine Vorreiterrolle für die öffentliche Verwaltung einnehmen;

   h) für Start-ups sollten in den ersten vier Jahren ihres Bestehens grundsätzlich wachstumsfördernde Sonderregeln gelten;

   i) für die Wachstumsphase von Unternehmen sowie KMU braucht es zusätzlich Unterstützung, insbesondere im Bereich der internationalen Skalierung und Digitalisierung;

   j) eine Initiative „Start-ups Digitale Wirtschaft“ zur Förderung von IKT-B2B-Start-ups (IKT = Informations- und Kommunikationstechnik; B2B = Business-to-Business) sollte ins Leben gerufen werden?

11. Mit welchen konkreten Zielen und Vorhaben hinterlegt die Bundesregierung die folgenden Forderungen aus dem Papier „Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen“, und welche konkreten Maßnahmen hat sie diesbezüglich bereits ergriffen:

   a) Kommunikationsnetze müssen jederzeit verfügbar sein, Menschen, Wirtschaft und Staat eine abhörsichere Kommunikation ermöglichen und Schutz vor Manipulation der transportierten Daten bieten;

   b) die erste Grundvoraussetzung für zuverlässige digitale Infrastrukturen ist vertrauenswürdige Technologie;

   c) Pfeiler für zuverlässige digitale Infrastrukturen ist die Kontrolle über nationale Telekommunikationsnetze, die zwingend in deutscher oder mindestens europäischer Hand sein müssen;

d) in Krisenfällen muss auch der physische Zugriff auf Rechenzentren gewährleistet sein;

e) da Digitalisierung im Allgemeinen auf die Speicherung von Daten angewiesen ist, müssen Cloud-Rechenzentren in Europa als kritische Infrastrukturen betrachtet werden;

f) damit IT-Sicherheit „made in Europe“ bestehen kann, brauchen heimische Anbieter öffentlich geförderte Leuchtturmprojekte;

g) europäische Initiativen zur Standardisierung von Security by Design und Security by Default müssen vorangetrieben werden;

h) für Aufbau und Erhalt digitaler Souveränität sind digitale Kompetenzen sowie die Fähigkeit, sichere Künstliche Intelligenz zu entwickeln, erforderlich;

i) Kontroll- und Innovationsfähigkeit müssen dadurch gesichert werden, dass kritische Daten der Verwaltung nur in Systemen verarbeitet werden, bei denen staatliche Organe die Hoheit darüber haben, wer auf diese Daten zugreifen kann und bei denen Daten jederzeit in andere Systeme übertragbar und durchsetzbar im ursprünglichen System löschbar sind;

j) bei öffentlichen Beschaffungen sollten Software- und Cloud-Angebote grundsätzlich bevorzugt werden, deren Quellcode geprüft und geändert werden kann; bei kritischen Systemen sollte dies verpflichtend sein?

Die Fragen 8 und 11 werden gemeinsam beantwortet.

Zudem wird auf die Antworten zu den Fragen 4, 5 und 6 verwiesen.

Die in den Papieren enthaltenen Handlungsempfehlungen werden von den zuständigen Ressorts sorgfältig geprüft und es werden – soweit möglich – geeignete Umsetzungsmaßnahmen ergriffen. Über die in den Antworten zu den Fragen 4, 5 und 6 aufgeführten Maßnahmen hinaus hat die Bundesregierung beispielsweise die folgenden Maßnahmen ergriffen, wobei die Liste nicht als erschöpfend betrachtet werden kann.

- Die Bundesregierung hat sich mit der IT-Konsolidierung Bund (Kabinettbeschluss vom 20. Mai 2015) zum Ziel gesetzt, die IT-Sicherheit vor dem Hintergrund steigender Komplexität zu gewährleisten, die Hoheit und Kontrollfähigkeit über die eigene IT dauerhaft zu erhalten, auf innovative technologische Trends flexibel reagieren zu können, einen leistungsfähigen, wirtschaftlichen, stabilen und zukunftsfähigen Betrieb sicherzustellen und ein attraktiver Arbeitgeber für IT-Fachpersonal zu bleiben. Die Daten der Bundesverwaltung sollen ferner umfassend geschützt und gegen Missbrauch abgesichert werden. Im Rahmen der IT-Konsolidierung Bund wurden die IT-Architekturrichtlinien des Bundes erarbeitet und durch den IT-Rat verabschiedet. Dort wird mit der Cloud-First-Vorgabe die Nutzung der Bundescloud grundsätzlich verpflichtend vorgegeben. Die Bundescloud wird als IT-Maßnahme der IT-Konsolidierung Bund aufgebaut. Seit Mitte 2017 ist die Bundescloud innerhalb des sicheren Behördennetzes (Netze des Bundes) für die Bundesbehörden nutzbar. Die Bundescloud soll als Private Cloud des Bundes insbesondere dessen hohe Informationssicherheitsanforderungen erfüllen und ist daher nicht aus öffentlichen Netzen erreichbar. Bundesbehörden können zudem auch Public-Cloud-Angebote nutzen. Voraussetzung dafür ist, dass kein entsprechender Cloud-Dienst in der Bundescloud angeboten wird und der „Mindeststandard des BSI zur Nutzung externer Cloud-Dienste“, der Beschluss des IT-Rats „Kriterien für die Nutzung von Cloud-Diensten der IT-

Wirtschaft durch die Bundesverwaltung“ sowie des darauf aufbauenden Beschlusses des IT-Planungsrats „Vorgehensweise und Kriterien zu Inanspruchnahme und Beschaffung von Cloud-Diensten der IT-Wirtschaft“ eingehalten werden.

- Hinsichtlich der in der Fragestellung erwähnten Kategorisierung von Cloud-Rechenzentren ist zunächst festzuhalten, dass in der Europäischen Union die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (sog. NIS-Richtlinie) gilt. In Artikel 4 Nummer 4 in Verbindung mit Anhang II der NIS-Richtlinie werden die Sektoren der „Betreiber wesentlicher Dienste“ definiert bzw. benannt. In Deutschland werden diese Dienste als Kritische Infrastrukturen nach § 2 Absatz 10 des BSI-Gesetzes erfasst. Eine davon zu unterscheidende Kategorie bilden die „digitalen Dienste“. Nach Artikel 4 Nummer 5 in Verbindung mit Anhang III der NIS-Richtlinie gehören hierzu Cloud-Computing-Dienste. Davon abgesehen fördert die Bundesregierung mit dem „International Data Space“ Technologien für den sicheren Datenaustausch in der Industrie 4.0. Technologische Grundlagen werden zudem im Rahmen des Forschungsrahmenprogramms der Bundesregierung „Selbstbestimmt und sicher in der digitalen Welt“ gelegt. Hierzu wird auf die Antwort zu Frage 5 verwiesen.

- In Bezug auf die Betreiber von Telekommunikationsnetzen gilt, dass diese im Zuge der Umsetzung der NIS-Richtlinie und auf Grundlage des IT-Sicherheitsgesetzes als Betreiber Kritischer Infrastrukturen bestimmt wurden. Diese Betreiber haben u. a. Maßnahmen zur Wahrung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme zu erbringen und gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bzw. der Bundesnetzagentur regelmäßig nachzuweisen.

- Im Zuge der Umsetzung der NIS-Richtlinie und ebenfalls auf Grundlage des IT-Sicherheitsgesetzes wurden zudem in Deutschland Rechenzentren bei Überschreitung bestimmter Schwellenwerte als kritische Infrastrukturen festgelegt.

- Die Aufklärungs- und Unterstützungsmaßnahmen der Initiative „IT-Sicherheit in der Wirtschaft“ schließen u. a. ein, Unternehmensleitung und Mitarbeiterinnen und Mitarbeiter bezüglich bestehender Risiken bei der Kommunikation im Netz zu sensibilisieren und Empfehlungen zu formulieren, wie diese Risiken wirkungsvoll minimiert werden können.

- Die Bundesregierung hat sich aktiv in die Verhandlungen zu der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 eingebracht. ENISA verfügt damit über ein zeitlich unbefristetes und inhaltlich erweitertes Mandat. Zudem wurden mit der Verordnung die Voraussetzungen für einen signifikanten Personalzuwachs geschaffen, wodurch insbesondere neue Aufgaben im Bereich der Zertifizierung wahrgenommen werden können.

- In der KI-Strategie der Bundesregierung verankert ist das Vorhaben einer vertrauenswürdigen Daten- und Analyseinfrastruktur einschließlich des Aufbaus einer zugrundeliegenden Cloud-Plattform. Derzeit werden Möglichkeiten zur Umsetzung im Dialog zwischen Staat, Wissenschaft und Wirtschaft geprüft, konkrete Daten sind daher aktuell nicht verfügbar.
- Der private Wagniskapitalfondsmarkt in Deutschland und Europa hat sich erheblich weiterentwickelt. So gibt es auch in Deutschland immer mehr Fonds mit einem Volumen von über 300 Mio. Euro, die Start-ups bei ihrem Wachstum begleiten. Die Dachfonds-Instrumente der Bundesregierung, wie der ERP/EIF-Dachfonds, die ERP-VC-Fondsinvestments und der Mezzanin-Dachfonds Deutschland beteiligen sich an dieser neuen Generation von Wachstumsfonds und hebeln so das private Engagement mit öffentlichen Mitteln deutlich. Im Fokus sind dabei auch sog. Venture-Debt-Fonds, die das Bindeglied zwischen dem klassischen Wagniskapitalmarkt und dem etablierten Kapitalmarkt bilden. Sie stellen schnell wachsenden Start-ups, die noch keinen Zugang zu klassischen Bankkrediten haben, Fremdkapital zur Verfügung.

  Ergänzend hat die Bundesregierung gemeinsam mit der Kreditanstalt für Wiederaufbau (KfW) Ende letzten Jahres das Programm „Venture Tech Growth Financing" gestartet, das zu 95 Prozent durch den Bundeshaushalt abgesichert wird. Auf diese Weise sollen Venture-Debt-Finanzierungen mit einem Gesamtvolumen von mindestens 500 Mio. Euro für Start-ups bereitgestellt werden.

  Zudem hat die Bundesregierung zusammen mit dem Europäischen Investitionsfonds (EIF) speziell für Technologieunternehmen in der Wachstumsphase die ERP/EIF-Wachstumsfazilität aufgelegt, die ein Volumen von 500 Mio. Euro hat.

  Die internationale Skalierung junger Unternehmen unterstützt die Bundesregierung auch durch den German Accelerator. An den Standorten Silicon Valley, New York, Boston und Singapur wurden bislang rund 230 deutsche Start-ups bei ihren Aktivitäten z. B. zur Markterschließung, Partnersuche oder Investorengewinnung unterstützt. Darunter waren namhafte Start-ups wie z. B. Celonis oder N26.
- Das BMBF fördert die Ausgründung von IKT-Start-ups aus Hochschulen und Forschungseinrichtungen mit technologiespezifischen Maßnahmen. So wurden an den Kompetenzzentren für IT-Sicherheit in Saarbrücken, Darmstadt und Karlsruhe sowie an der Ruhr-Universität Bochum Gründungsinkubatoren aufgebaut und es werden gezielt Gründungsprojekte gefördert. Ähnliche Maßnahmen hat das BMBF auch in anderen Technologiefeldern aufgelegt, etwa in der Mikroelektronik und der Photonik.
- Die Digital Hub Initiative des BMWi wurde u. a. zur Förderung von IKT-B2B-Start-ups ins Leben gerufen. Ziel ist es, die Vernetzung der zwölf ausgewählten Digital Hubs untereinander zu stärken und sie international sichtbarer zu machen. In den Hubs werden deutsche und internationale IKT-B2B-Start-ups mit Wissenschaftlerinnen und Wissenschaftlern, Investoren und etablierten, möglichst mittelständischen, Unternehmen zusammen gebracht, um gemeinsam Antworten auf die Herausforderungen des digitalen Zeitalters zu finden.

- Die Entwicklung sicherer KI ist ein zentrales Ziel der KI-Strategie der Bundesregierung. Das BSI beabsichtigt, Forschung im Bereich sichere KI durchzuführen, unter anderem bezüglich der Analyse von Angriffen auf KI-Systeme und die Entwicklung von entsprechenden Abwehrmaßnahmen. Diese Forschungsmaßnahmen werden im Rahmen der KI-Strategie der Bundesregierung durchgeführt und sollen nach Abschluss veröffentlicht werden.
- Das BMWi fördert im Rahmen der „Smart Service Welt II" das F&E-Projekt „OPTIMOS 2". Ziel von OPTIMOS 2 ist die Entwicklung eines offenen praxistauglichen Ökosystems für sichere Identitäten auf dem Smartphone. Die Erprobung erfolgt mit der sicheren Speicherung einer vom deutschen Personalausweis abgeleiteten Identität auf dem Smartphone, welche anschließend in unterschiedlichsten Szenarien eingesetzt werden kann, z. B. im ÖPNV, beim Check-in im Hotel, beim Carsharing etc.

9. Wie soll nach Ansicht der Bundesregierung das Ziel erreicht werden, dass auch europäische Plattformen globale Standards setzen können und in ihren Bereichen die Marktführerschaft einnehmen?

   Welche Wachstumshürden bestehen für Unternehmen nach Ansicht der Bundesregierung durch die Verantwortlichkeit für Inhalte, die Plattformbetreibern mit der Urheberrechtsrichtlinie (Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt) auferlegt werden?

Digitalisierung der Industrie und das Internet der Dinge große Chancen für Deutschland und seine Unternehmen, erfolgreiche digitale Plattformen auf den Markt zu bringen – allem voran im Bereich Business to Business. Damit diese Chancen genutzt werden können, sollte die Regulierung existierender Plattformen keine Eintrittshürden für aufstrebende deutsche und europäische Geschäftsmodelle, sondern ein wettbewerbsfähiges Umfeld für Plattformen aus Deutschland und Europa schaffen.

Außerdem muss sichergestellt werden, dass den deutschen und europäischen Plattformen ausreichend Kapital für das schnelle und dynamische Hochskalieren ihres Geschäftsmodells zur Verfügung steht. Auch hierfür hat die Bundesregierung zusammen mit der KfW Ende letzten Jahres das Programm „Venture Tech Growth Financing (VTGF)" im Rahmen der „Tech Growth-Fund"-Initiative gestartet, mit dem Unternehmen in der Wachstumsphase Zugang zu sog. Venture-Debt-Finanzierungen erhalten sollen. Des Weiteren haben das BMWi, das Bundesministerium der Finanzen und die KfW gemeinsam die Beteiligungsgesellschaft KfW Capital aufgesetzt. KfW Capital strebt in den nächsten zehn Jahren ein Zusagevolumen von insgesamt 2 Mrd. Euro an.

Artikel 17 der Richtlinie über das Urheberrecht und die verwandten Schutzrechte im Digitalen Binnenmarkt regelt die Verantwortlichkeit bestimmter Plattformen für von Nutzerinnen und Nutzern hochgeladene urheberrechtlich geschützte Inhalte. Diese Vorschrift richtet sich ausschließlich an Plattformen, die der Öffentlichkeit eine große Menge urheberrechtlich geschützter Werke zugänglich machen. Ausgenommen hiervon sind unter bestimmten Voraussetzungen Start-ups in den ersten drei Jahren ihrer Geschäftstätigkeit. Der Grundsatz der Verhältnismäßigkeit ist zu beachten. Die Bundesregierung hat ihre Maßgaben für die Umsetzung der Vorschrift in der Protokollerklärung vom 15. April 2019 formuliert (verfügbar unter https://data.consilium.europa.eu/doc/document/ST-7986-2019-ADD-1-REV-2/de/pdf).

10. Inwiefern wird bei der IT-Beschaffung durch die Bundesregierung das Prinzip der digitalen Souveränität und die Kriterien des im Papier „Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen“ erarbeiteten Schichtenmodells berücksichtigt?

Es wird auf die Antworten zu den Fragen 5, 8 und 11 verwiesen.

12. Wie sollen nach Ansicht der Bundesregierung Deutschland und Europa, die aktuell als Standorte für Rechenzentren aufgrund der vergleichsweise hohen Stromkosten eher unbeliebt sind, zu attraktiveren Standorten für Rechenzentren werden?

Es ist zutreffend, dass die Strompreise in Deutschland im europäischen und internationalen Vergleich hoch sind. Das gilt allerdings nicht für die besonders stromintensive Industrie, welche von bestimmten Entlastungen profitiert, um ihre internationale Wettbewerbsfähigkeit zu wahren.

Grundsätzlich ist es das Ziel der Bundesregierung, quer durch sämtliche Industriesektoren hinweg wettbewerbsfähige Strompreise für die Industrie zu gewährleisten und einen weiteren Anstieg der Strompreise zu vermeiden. Dafür ist es wichtig, die Energiewende so kosteneffizient wie möglich zu gestalten. Deswegen hat die Bundesregierung beispielsweise die Umstellung der EEG- und KWK-Förderung auf wettbewerbliche Ausschreibungen vorgenommen. In der Folge konnte die EEG-Umlage dieses und letztes Jahr jeweils leicht gesenkt werden. Dies kommt auch den Betreibern von Rechenzentren zugute.

Darüber hinaus sind auch weitere Standortfaktoren relevant für die Ansiedlung von Rechenzentren in Deutschland. Hierzu zählen beispielweise neben der Sicherheit der Stromversorgung auch die geltenden Datenschutzbestimmungen, die allgemeine Rechtssicherheit am Standort Deutschland, die Konnektivität sowie auch räumliche Nähe zu den Kunden, um große Latenzen zu vermeiden.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333